Formation T.I.C.

Bibliothèque Départementale de Prêt de la Dordogne

SECURISER SON ORDINATEUR

Formation

Bibliothèque Départementale de prêt de la Dordogne
Service de l'informatique documentaire et des T.I.C
Animateurs – Formateurs : ***Olivier Dutard – Christelle Lozach***
Tél : 05 53 53 65 56 ou 05 53 53 37 82

Sommaire

Pourquoi la sécurité informatique ?

Tout comme vous fermez la porte de votre domicile, il convient de verrouiller un minimum votre ordinateur afin que ce ne soit pas une porte ouverte à toute intrusion.
L'internaute est responsable de la bonne santé de son ordinateur, que ce soit pour l'intégrité de ses données mais aussi pour les autres internautes, l'internaute doit en conserver la maîtrise (ce qui demande un minimum de connaissance technique).

Imaginez un instant de la vulnérabilité de votre réseau, du matériel informatique, des ordinateurs, des menaces internes et externes (anti-virus, troyens, spams, pop ups, cookies etc.)
La sécurité est primordiale, il en va de la crédibilité et de la survie de votre travail, de votre outil personnel et professionnel...

Imaginez que votre collègue, votre voisin, un client ou un inconnu mal intentionné reçoivent votre carnet d'adresses ou des documents confidentiels (documents internes, photos personnelles, factures...). Tout ceci à votre insu, par le tout dernier virus à la mode, par un troyen, spyware ou autres qui s'est introduit dans votre système informatique.

Des pertes de données ne sont pas exclues...

Prenez conscience du danger que représente un ordinateur, voire un réseau informatique non protégé. Avec Internet Haut débit, les conséquences s'en trouvent démultipliées.

Savez vous qu'un ordinateur non protégé avec une connexion Internet, peut être contaminé au bout de 17 minutes environ !

Quels sont les risques et les menaces ?

Lorsque vous naviguez sur Internet, ou téléchargez et installez des programmes, vous devez être vigilants. En effet, des pièges ou arnaques sont monnaie courante sur la toile.

Pour infecter des ordinateurs, les moyens de propagations qui pourront toucher le plus de monde possibles passent le plus souvent par Internet, c'est à dire :

- **Des programmes piégés sur des sites de téléchargement** :
  l'internaute télécharge et lance des exécutables (.exe ; .zip ...) depuis des sites de téléchargements ou depuis des Réseau « Pear to pear ».

- **Des logiciels installant des logiciels tiers** comme les adwares.
  Les adwares sont des virus qui "ajoute" des activités indésirables sur votre ordinateur. Par exemple, une fenêtre qui s'ouvre toute seule pour de la publicité même si votre page Internet est fermée. Ou encore, un programme ou un logiciel qui s'active au démarrage. Ils peuvent changer toute votre configuration, dépendant de la gravité de l'adware.

- **Les fausses alertes de sécurité** qui vous proposent d'installer de faux anti-spywares (dits "rogues") lors de l'accès à certains sites.

- Les **mails infectés** et des hoax (canulars du net).

- Des **programmes alléchants piégés**.

- Des messages vous demandant d'aller sur des **sites piégés** sur les newsgroups, forums et réseaux IRC.

N'ouvrez pas n'importe quel fichier, faites attention à ce que vous téléchargez et d'où vous téléchargez.

Lorsqu'un ordinateur est infecté par un trojan, il est à la merci d'un pirate ou d'une organisation. Ce dernier peut faire tout ce qu'il désire avec cet ordinateur même en étant à des milliers de kilomètres.

Vos données personnelles : mot de passe, documents Word & Excel ne sont plus à l'abri puisque ce dernier peut les modifier ou supprimer.
Lorsque le PC est infecté et à la merci d'un pirate, on dit alors que c'est un **PC zombie**.

La législation sur la sécurité informatique :

L'utilisateur de systèmes informatiques, le pirate et le fournisseur de produits informatiques sont trois acteurs clés du débat sur la sécurité informatique.

Il n'existe à l'heure actuelle aucune législation véritablement internationale concernant la criminalité informatique. Un pirate pourra donc avoir un accès non autorisé à un système informatique se trouvant à l'étranger sans être trop inquiété par la justice.

Actuellement, plusieurs textes sont en préparation, dans l'objectif de renforcer l'arsenal existant contre la fraude informatique. Ces textes pourraient avoir pour conséquence d'incriminer dans le même temps des actes destinés à l'amélioration de la sécurité des systèmes d'information.

Les pratiques à risques : « portrait d'un utilisateur à risques »

- **Avoir une trop grande confiance** voire une confiance aveugle dans les outils de protection (antivirus et firewall).
  Un antivirus est loin d'être infaillible. On dit même qu'actuellement les pirates ont pris une sérieuse avance sur les antivirus qui ont depuis quelques années peut évoluer, notamment en ce qui concerne les ***rootkit***.

- Suite à une infection, le seul réflexe de l'internaute est de demander "Quel est le meilleur antivirus" et ne se pose pas la question : ***pourquoi et comment j'ai été infecté ?***

- **L'installation à tout va de logiciel sans en vérifier l'authenticité** et la source. Ceci peut être généralement des sources dangereuses : Réseau P2P , Site Web non vérifié, etc..
  Par exemple : Mon antivirus ne détecte rien sur le logiciel installé depuis une source dangereuse. Vous en concluez que le logiciel n'est pas dangereux ! Grave erreur !
  N'installez que des programmes depuis des sources sûres : 01net, zebulon, zdnet, clubic, infos-du-net ou les sites de vos fournisseurs d'accès.

- En général la seule solution de sécurité trouvée par la majorité des internautes est de multiplier les logiciels de protection, on retrouve souvent plusieurs antispywares (SpyBot, Ad-aware, AVG Antispyware, Spyware Terminator) sur une même machine croyant que cela les protègera mieux.
  - Les résultats sont plutôt médiocres et mitigés.
  - De plus, cela ralenti considérablement l'ordinateur.

Ce que vous devez comprendre, c'est que votre antivirus ne détecte qu'à peine 1/3 des programmes dangereux, la seule parade est la **méfiance**.

N'installez pas le premier programme venu, n'exécutez pas le premier fichier venu même si votre antivirus ne dit rien.

Connaître les différentes familles de virus et les menaces informatiques.

Un virus est un petit programme conçu pour se cacher dans votre ordinateur, puis se multiplier, se répandre de par le monde et enfin déclencher une action (message, destruction, petite musique, etc.). On dénombre plusieurs catégories de virus, en fonction de la cible visée dans l'ordinateur.

Les différentes familles de virus

- La première catégorie regroupe les **virus de secteur d'amorce** (= virus de "boot sector", c'est-à-dire affectant la zone du disque qui est lue en premier au démarrage) tels que Form, jack the ripper, french boot, parity boot... Ces virus remplacent le secteur d'amorce du disque infecté par une copie d'eux-mêmes, puis déplacent le secteur original vers une autre portion du disque. Le virus est ainsi chargé en mémoire bien avant que l'utilisateur ou un logiciel ne prenne le contrôle de l'ordinateur.
- Les **virus d'application** infectent les fichiers exécutables, c'est-à-dire les programmes (.exe, .com ou .sys). Pour simplifier, disons que le virus remplace l'amorce du fichier, de manière à ce qu'il soit exécuté avant le programme infecté, puis il lui rend la main, camouflant ainsi son exécution aux yeux de l'utilisateur.
- Les **virus macro** sont des virus qui infectent uniquement des documents (Word, Excel…). Ces virus se propagent actuellement dans de fortes proportions et peuvent malheureusement causer de grands dégâts (formatage du disque dur par exemple).
- Enfin, il y a les **virus de mail**, également appelés **vers**. Ces virus se servent des programmes de messagerie (notamment Microsoft Outlook) pour se répandre à grande vitesse, en s'envoyant automatiquement à tout ou partie des personnes présentent dans le carnet d'adresses. Leur premier effet est de saturer les serveurs de messagerie, mais ils peuvent également avoir des actions destructrices pour les ordinateurs contaminés. Ils sont particulièrement redoutables, car le fait de recevoir un mail d'une personne connue diminue la méfiance du destinataire, qui ouvre alors plus facilement le fichier joint contaminé.

A noter que certains virus sont des virus polymorphes. A chaque fois que l'un d'eux infecte un fichier, il se crypte différemment. Résultat, il faut que l'antivirus analyse la technique d'encryptage de chaque virus pour déceler, dans les fichiers contaminés, une sorte de "manie" caractéristique, une constante.

Il ne faut pas confondre les virus avec les troyens ou les emails bombs. Contrairement à son cousin le virus, qui profite de toute occasion pour se multiplier, le troyen véritable ne se reproduit pas. Par ailleurs, plusieurs vulnérabilités dans les logiciels Internet Explorer / Outlook font que certains virus peuvent infecter votre ordinateur à la simple ouverture du message ou lors de sa lecture dans la fenêtre de visualisation voire en consultant une page.

Les **spywares** sont des logiciels qui espionnent surtout votre comportement pour vous situer comme consommateur. Leur nombre envahissant finit par ralentir à l'extrême votre ordinateur. De plus, niché au milieu de ces milliers d'espions d'autres peuvent détourner vos données confidentielles, privées ou commerciales.

Ce fléau toucherait 90 % des ordinateurs connectés au réseau mondial. En à peine deux ans, plus de 30 000 spywares ont fait leur apparition.

Connaître les outils de protection

Il n'existe pas de protection absolue et c'est pourquoi il est recommandé de mettre en place un système de sauvegarde sécurisé pour vos données importantes tel un disque dur externe de grande capacité (connecté sur un port USB et déconnecté entre les sauvegardes). Une clé USB peut suffire selon le volume de données que vous avez à protéger. Dans les cas extrêmes on peut sauvegarder sur des supports (cdrom, disquette).

Les logiciels gratuits désignés ci-après le sont à titre d'information et se trouvent en ce moment sur Internet. Ils ne concernent que les particuliers et n'offrent pas de degré de protection absolue.

L'idéal pour les sauvegardes c'est de ne pas avoir à être utilisées, c'est pourquoi nous vous recommandons également un bon anti-virus et un bon pare-feu. D'autres solutions comme les anti-spywares sont aussi utilisables.

ANTIVIRUS

Bien choisir ses logiciels, maintenir son système et ses applications le plus à jour possible, fermer le maximum de points d'entrée, se méfier des mails et des liens web, c'est la première étape pour éviter les ennuis pour soi, mais aussi les autres. Malheureusement, comme il existe toujours des imperfections dans le système ou dans les applications, il faut encore ajouter des verrous et s'équiper pour le nettoyage en cas d'intrusion. C'est le rôle des anti-virus.
Les **antivirus** vous permettent de protéger votre pc contre les attaques de virus qui peuvent venir d'internet, des e-mails (courriel à la française) ou de CD infectés. Le problème c'est que de nouveaux virus apparaissent régulièrement et qu'il est impossible d'être protégé à 100%.
Les bases de données des nouveaux anti-virus sont mises à jour très fréquemment.
Parmi les gratuits on trouve **Antivir**, AVG et **Avast!** Ils sont gratuits pour un usage personnel.

PARE-FEUX

Les **pare-feux (firewalls)** protègent des intrusions sur votre pc par des programmes inconnus et non sollicités qui peuvent infecter votre micro avec un virus « cheval de troie » ou autre, et éventuellement pirater vos données. Ils sont programmés pour surveiller tout le trafic internet de votre PC et ne laissent passer que les programmes que vous autorisez tel Internet Explorer etc.

Les firewalls matériels

Les firewalls matériels protègent tout le réseau local et les firewalls logiciels ne protègent que la machine sur laquelle ils sont installés.

Optez pour un firewall logiciel si vous ne possédez qu'une machine, mais adoptez les « deux » solutions si vous avez un réseau. En jargon technique, l'usage de 2 firewalls s'appelle une « **défense en profondeur** ». Elle s'est imposée avec l'arrivée des réseaux sans fil. Le firewall matériel constitue un premier bouclier entre Internet et le réseau local (qu'il soit « sans fil » ou non).

Les firewalls logiciels

Le firewall logiciel incorporé dans Windows est suffisant pour la plupart des utilisateurs. Il protège très efficacement votre machine de toute attaque venue de l'extérieur. Mais il ne fournit aucun détail sur les attaques subies par la machine. Et surtout il ne protège pas des Trojans déjà présents sur l'ordinateur car il ne filtre pas ce qui sort de la machine.

Pare feu et antivirus sont deux choses distinctes mais les deux associés contribuent à protéger votre ordinateur.

ANTI-ROOTKIT

Un rootkit permet à quelqu'un d'accéder à distance à un ordinateur en tant qu'administrateur de la machine sans que l'utilisateur ne s'en rende compte. Ce type de logiciel peut être installé suite à une infection par un logiciel malveillant mais échappe souvent à des analyses de type anti-virus ou anti-spyware. La caractéristique principale d'un rootkit est la discrétion : ils savent se rendre invisibles !

ANTI-SPAM

Pour lutter contre les courriers électroniques non sollicités (spam, pourriel), de plus en plus de fournisseurs d'accès Internet proposent un service anti-spam. L'**anti-spamming** désigne un ensemble de systèmes et moyens techniques et juridiques de lutte contre les courriers électroniques publicitaires non sollicités (logiciels anti-spam).

Quelles précautions prendre pour assurer la sécurité de ses données ?

- **Créer un double de ses documents importants sur un autre support** (autre disque dur, cd, dvd, etc...)

- **Maintenir à jour ses copies** de sauvegarde

- Lorsque l'on **utilise des clés usb**, évitez de laisser des documents importants sans avoir une **autre copie en lieu sûr** (disque dur, cd, dvd, etc...). En effet, les clés usb peuvent être perdues facilement et surtout, montrent un manque de fiabilité. Si votre clé venait à défaillir, il est important d'avoir des copies sur un autre support.

- Si l'on a des données sur un ftp, ou un site personnel ou professionnel sur le net, le site peut être parfois inaccessible pour maintenance, par exemple. Si vous auvez besoin de vos fameuses données, ce jour là, vous seriez ennuyé (le risque de perte est faible, la plupart des services d'hébergement sérieux réalisent, toutefois, des sauvegardes des fichiers.).

En conclusion, le meilleur support pour conserver ses données, ce sont les disques de données comme les CD-R ou CD-RW (réinscriptible) ou les DVD-R ou DVD-RW (réinscriptible).

Que faire en cas d'infection ?

- Tout d'abord, ne pas céder à la panique!

- La première précaution (dans la mesure du possible) consiste à déconnecter votre pc du réseau (réseau domestique, d'entreprise, d'internet) afin d'empêcher l'infection de se répandre.

- Ensuite il faut (si possible) identifier le virus -probable- avec votre antivirus.

- Chercher le maximum d'information sur le virus en question, avec google ou sur les sites d'éditeurs d'antivirus *(voir plus bas pour la liste)* via un autre pc si possible.

- Si l'étape de l'indentification du virus est impossible, visitez un site proposant un antivirus en ligne *(liste plus bas).*

Note importante: Dans le cas où le virus est toujours actif (car non supprimé par votre antivirus, avant de réactiver votre connexion réseau pour faire un « scan » en ligne, il est important d'arrêter les processus suspects (via le gestionnaire des tâches, qui s'active en appuyant simultanément sur Ctrl – Alt – suppr).

- Réaliser le « scan » complet de la machine avec l'antivirus.

En cas de présence d'un malware introuvable ou résistant.

L'ordinateur présente tous les symptômes d'une infection virale mais aucun programme malsain n'est détecté lors des « scans » en ligne.

On est probablement confronté à un **rootkit (malware)** ayant la faculté de se cacher assez profondément.

Ainsi, un rootkit peut:

- Etre visible dans le gestionnaire des tâches (souvent sous un nom bizarre du type "ahrgvtx.exe), mais pas trouvable lors d'une recherche de fichiers sur le disque dur.
- Etre invisible dans le gestionnaire des tâches et dans ce cas, on peut utiliser un antirootkit pour le révéler.

Noter le nom du potentiel agent infectieux.

Redémarrer Windows en mode sans échec (appuyer sur F8 après le premier écran du BIOS, et choisir "mode sans échec" dans le menu affiché).

Rechercher sur le disque dur le probable **rootkit** (dont on aura noté le nom).

Une fois localisé, l'isoler (en lançant l'antivirus et en le mettant en quarantaine par exemple) ou le supprimer.
Noter d'ailleurs qu'il y a de fortes chances pour que l'antivirus détecte ce fichier comme étant un virus.

Ensuite, aller dans démarrer / exécuter, taper "msconfig" *(sans les guillemets).* Une fois dans msconfig, allez dans l'onglet démarrage, puis décochez la case correspondant au programme que l'on a localisé à l'étape précédente.

Pour être sûr d'avoir tout bien supprimé regarder s'il n'y a pas d'autre nom étrange dans msconfig / démarrage.

Faire une analyse antivirus en mode sans échec.

Une fois que tout ceci est fait, redémarrer le pc en mode normal, tout doit être rentré dans l'ordre.

Se protéger sur Internet

Conseils à mettre en application pour éviter une infection :

- Tout d'abord configurer correctement le système pour éviter les mauvaises surprises, et pour vous permettre de déterminer au mieux les risques d'infections.

- Ne jamais ouvrir de pièce jointe d'un mail paraissant étrange.

- Ne jamais oublier que le mail est la voie d'infection la plus répandu (surtout pour les virus.).

Voici quelques conseils :

Comme annoncé ci-dessus, ne jamais ouvrir de pièces jointes d'un courriel bizarre (comme un E-mail en anglais, par exemple, bien que certains virus puissent générer des messages incitant à ouvrir la pièce jointe en plusieurs langues)

Au niveau des pièces jointes, certains autres signes peuvent permettre de reconnaître une pièce jointe potentiellement dangereuse dont l'extensions de ces pièces jointes peuvent être:
Par exemple, .exe .bat .scr .htm .html .chm .com .pif .lnk .cmd .vbs .doc .xls

Toujours concernant les extensions, il est très important de faire attention à certaines pièces jointes qui possèderaient 2 extensions (ex : .jpg.exe).
Toute la subtilité est dans la seconde extension (vu qu'il y a dans le nom ".jpg", on pourrait penser qu'il s'agit d'une image, erreur). Les .exe doivent inciter à la plus haute méfiance car il s'agirait bien ici d'une application.

Autre problématique au niveau des extensions, Windows n'est pas configuré par défaut pour afficher la double extension, ce qui est susceptible d'induire en erreur.

De plus, éviter d'ouvrir des mails dont on ne connaît pas l'expéditeur : un mail peut tout comme une simple page Web contenir un script malintentionné, et dans ce cas, pas besoin de pièce jointe pour contaminer.

Pour ce qui est des mails : si on utilise un logiciel de messagerie (Outlook, Thunderbird, Foxmail ou autres...), le risque de mail infecté est potentiellement plus élevé. En fonction de la configuration de l'application de courrier, il est possible que le courrier filtré et placé dans « spam » par le service d'email téléchargé. Dans ce cas, les messages de spam et/ou infectés sont tout à fait visibles et ouvrables, donc prudence.

Hormis les mails, d'autres voix de contaminations existent.

La deuxième plus grande est le téléchargement de fichiers *:*

En effet, tous les fichiers téléchargés devraient être traités avec la même attention. Vous n'êtes jamais certains, que l'application que vous venez de télécharger, n'est pas en fait un virus déguisé (Sauf, bien sur si ce fichier provient d'un site réputé et sûr).

Dans un site réputé et sûr, le risque est beaucoup moins élevé mais jamais nul, en théorie.

Par ailleurs, les fichiers Word et Excel doivent être traités avec une grande méfiance : ils sont en effet susceptibles d'embarquer des virus macro, qui peuvent la aussi infecter votre machine.

Eviter aussi de surfer sur des sites warez[1], pornographiques, (…). Ils regorgent la plupart du temps de trojans, virus, spyware.

Lorsqu'un téléchargement "inopiné" est proposé, vous devez être très vigilant, car çela peut très bien être un programme utile (Flash player par exemple) ou un programme nuisible.

Certains logiciels installent des "spywares". *(Kazaa, par exemple)*

D'une manière plus générale, il faut éviter de télécharger « n'importe quoi » *(programmes, documents provenant d'une source non fiable)*.

Il est utile de prendre le temps de télécharger les mises à jour corrigeant des failles de sécurité pour vos logiciels, et notamment antivirus, *Windows (quand il vous demande de mettre à jour),* programmes en rapport avec Internet *(navigateur, logiciel servant à lire vos email, logiciel de discussions)*.

Sauvegarder régulièrement ses données les plus importantes *(cela permet en cas d'attaque virale de les récupérer si elles sont détruites et seront à l'abri en cas d'éventuelle panne matérielle.)*

[1] *Logiciels piratés (dont les protections ont été "crackées") disponibles sur des sites spécialisés et éphémères du fait de leur illégalité.*

Le Commerce électronique

Depuis sa création, le réseau Internet a tellement évolué qu'il est devenu un outil essentiel de communication. Cependant, cette communication met de plus en plus en jeu des problèmes stratégique liés à l'activité des entreprises sur le Web. Les transactions faites à travers le réseau peuvent être interceptées, d'autant plus que les lois ont du mal à se mettre en place sur Internet, il faut donc garantir la sécurité de ces informations, c'est la cryptographie qui s'en charge.

Qu'est-ce que la cryptographie ?

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe chiffrer.

Ceci permet :

- aux données d'être modifiées de telle façon à les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé cryptogramme (en anglais ciphertext) par opposition au message initial, appelé message en clair (en anglais plaintext) ;
- de faire en sorte que le destinataire saura les déchiffrer.

Le fait de coder un message de telle façon à le rendre secret s'appelle chiffrement. La méthode inverse, consistant à retrouver le message original, est appelée déchiffrement.

Les fonctions de la cryptographie

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

Le Protocole de sécurité SSL

SSL (Secure Sockets Layers) est un procédé de sécurisation des transactions effectuées via Internet.

Le standard SSL a été mis au point au départ par Netscape, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur internet. Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification.
De cette manière, SSL est transparent pour l'utilisateur. Par exemple un utilisateur utilisant un navigateur internet pour se connecter à un site de commerce électronique sécurisé par SSL enverra des données chiffrées sans aucune manipulation nécessaire de sa part.

La quasi intégralité des navigateurs supporte désormais le protocole SSL. Netscape Navigator affiche par exemple **un cadenas verrouillé** pour indiquer la connexion à un site sécurisé par SSL et un cadenas ouvert dans le cas contraire, tandis que Microsoft Internet Explorer affiche un cadenas uniquement lors de la connexion à un site sécurisé par SSL. 

Un serveur web sécurisé par SSL possède une URL commençant par https://, où le "s" signifie bien évidemment secured (sécurisé).

La transaction sécurisée par SSL se fait selon le modèle suivant :

- dans un premier temps, le client se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier.
- le serveur a réception de la requête envoie un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA), ainsi que le nom du cryptosystème.
- le client vérifie la validité du certificat (donc l'authenticité du marchand), puis crée une clé secrète aléatoire et chiffre cette clé.
- le serveur est en mesure de déchiffrer la clé avec sa clé privée. Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs.

Attention au piratage des mots de passe

De nos jours, on utilise beaucoup de mots de passe pour accéder à nos mails, chatter, accéder à nos fichiers, régler nos factures mais il n'est pas évident de retenir tous ces codes d'accès. Certains ont tendance à utiliser le même mot de passe partout. Malheureusement, Ceci est une très mauvaise idée car si un pirate parvient à trouver votre mot de passe, il aura accès à tout.
A l'inverse, quand on protège ses données avec des mots de passe différents, on a rapidement tendance à les oublier.
Certains choisissent des mots de passe trop simples devient plus facile pour les hackers de les deviner.
D'autres laissent les logiciels retenir leurs mots de passe, ce qui peut-être dangereux car le piratage est possible, et en cas de problème (plantage, réinstallation) sachez que vous pouvez perdre tous vos mots de passe.

Idéalement, un bon mot de passe est long (plus de 8 caractères) et mélange lettres, chiffres et symboles.

Alors comment choisir un mot de passe assez complexe mais facile à retenir ?

Voici une méthode efficace :
- Choisissez une phrase
- Prenez la première lettre de chaque mot
- Ajouter quelques chiffres et symboles.

Un exemple :
La **V**ie **E**st **U**n **L**ong **F**leuve **T**ranquille
Ce qui donne: **lveulft**
On peut ensuite ajouter chiffres (votre mois ou année de naissance) et symboles: lveu**72**lft**&&**

De cette manière, le mot de passe est long et pratiquement inattaquable et vous pourrez le retrouver assez facilement à partir de la phrase.

Un mot de passe différent pour chaque site.

Il ne faut jamais utiliser le même mot de passe sur différents sites.

Il y a moyen, à partir de la méthode précédente, d'avoir un mot de passe différent pour chaque site: Vous pouvez utiliser une phrase en rapport avec le site, par exemple: "*J'adore mon imprimante Canon EOS 300D*" sur Flickr.com, "*Gare aux virus sur des messages douteux*" sur outlook, etc.

Autre solution: utiliser une partie du nom de domaine dans votre mot de passe.

Par exemple, si votre mot de passe est lveu**72**lft**&&** utilisez :

- **f**lveu72lft&& sur **f**lickr.com
- lveu72lft**c**&& sur **c**ommentcamarche.net

Sécuriser l'environnement pour les enfants

Filtres enfants

Les filtres enfants offre la possibilité de bloquer les contenus adulte ou choquants.

Voici 3 applications qui peuvent vous aider à protéger vos enfants sur internet :

. Naomi

. LogProtect

. OpenDNS *(ne nécessite l'installation d'aucun logiciel.)*

Attention : Il faut bien garder à l'esprit que ces logiciels ne suffisent pas. Ils ne remplacent en **aucun cas** une supervision de l'utilisation d'internet par un adulte. Vous *devez* être présent et accompagner votre enfant quand il va sur internet.

Malgré tout, ces logiciels pourront vous apporter une aide supplémentaire. Ces trois logiciels sont entièrement gratuits, simples à utiliser et complémentaires.

Contrôle parental

Tous les fournisseurs d'accès à Internet proposent un logiciel de contrôle parental gratuit.

Il fonctionne généralement à l'aide de 3 profils :

- Enfant (moins de 10 ans).

En choisissant le profil « enfant », votre enfant naviguera dans un univers fermé, dit « liste blanche ». Il n'aura accès qu'à une sélection de sites (plusieurs milliers) prédéfinis correspondant à ses centres d'intérêt.

- Ado (plus de 11 ans).

En choisissant le profil « adolescent », votre enfant aura accès à tout Internet mais les sites illégaux (racisme, drogue…) et inappropriés (pornographie, violence…) seront filtrés à l'aide d'une liste noire.

- Adulte (les parents)

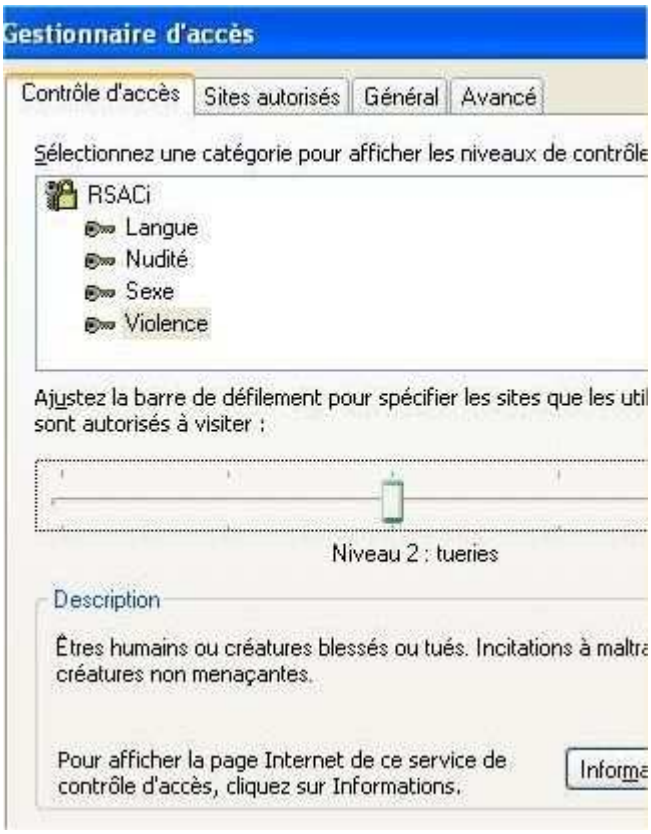
Les logiciels de ***contrôle parental*** permettent également de bloquer les chats, les forums, les jeux interdits aux mineurs, les téléchargements de vidéo, de musiques (souvent illégaux) et de limiter les horaires de connexion à Internet.

La meilleure sécurité pour les enfants réside dans le dialogue avec eux. Aucun logiciel de contrôle parental ne leur assurera une sécurité totale. Le logiciel de contrôle parental doit seulement être considéré comme un outil d'aide dans l'éducation sur Internet.

Pour plus d'infos sur l'efficacité des logiciels de contrôle parental proposés par les fournisseurs d'accès à Internet :
http://www.e-enfance.org/cote_parents/soft/test/

Paramétrer le contrôle parental de votre navigateur Internet Explorer

Pour utiliser Internet Explorer comme logiciel de filtrage de contenu, il est nécessaire d'activer son gestionnaire d'accès en sélectionnant la fonction Options Internet... dans le menu Outils.



La fenêtre Options Internet apparaît.

Cliquez sur le bouton de commande Activer, accessible à partir de l'onglet Contenu. Internet Explorer propose par défaut le système de filtrage de l'IRCA, organisme de classification de sites web, qui s'appuie en partie sur le PICS.
Le système de protection mis au point par l'ICRA classe les sites jugés embarrassants ou non suivant quatre critères: langue, nudité, sexe, violence. Les sites référencés disposent d'une étiquette en rapport.
Par exemple en saisissant l'adresse « porno.com » sous Internet Explorer, son gestionnaire d'accès indiquera que le site obtient les notes maximales en termes de violence, langage et caractère sexuel.

Pour chacune des catégories, il est nécessaire de déplacer la barre de défilement en fonction du niveau de protection souhaité.
Le niveau 0 étant le plus restrictif.
Un mot de passe Superviseur est exigé. Il doit être conservé précieusement, puisqu'il est exigé lors de la modification des paramètres de filtrage ou lors de l'affichage de page web non conformes.

Tout site n'intégrant pas d'étiquette PICS dans l'entête de ces pages ne pourra pas s'afficher sans autorisation. Malheureusement, c'est le cas d'un bon nombre de sites web. Il suffit pour s'en rendre compte de saisir l'adresse de sites web dans **l'outil de vérification de l'ICRA.** Dans la plupart des cas, une boîte de dialogue sous Internet Explorer invitera à autoriser ou interdire l'accès de ces sites au fur et à mesure de la navigation.

Utiliser son navigateur internet comme outil de filtrage ne peut être qu'une solution partielle, puisqu'il ne surveille que le contenu de sites internet et non les autres canaux tels que la messagerie instantanée et les logiciels de partage de fichiers.

Alice
L'option contrôle parental se trouve en bas de la page d'accueil. Cliquez sur « contrôle parental ». Une fois que vous êtes sur la page dédiée au contrôle parental, identifiez-vous (rentrez votre adresse mail ainsi que votre mot de passe) afin de recevoir le logiciel.
http://www.aliceadsl.fr/securitepc/default_copa.asp

Club Internet
Pour trouver l'option contrôle parental , cliquez en haut de la page d'accueil sur « Déjà abonné ? Identifiez-vous ». Identifiez-vous en entrant votre login et votre mot de passe. Allez ensuite dans la rubrique « Sécurité » et cliquez sur « contrôle parental ».
http://adsl.club-internet.fr/television/securite.phtml?opt=par

Free
L'option contrôle parental se trouve en bas de la page d'accueil. Cliquez sur « Protection de l'enfance ». Une fois que vous êtes sur la page dédiée au contrôle parental, cliquez sur « Installation de Free Angel Beta ». Vous n'avez pas besoin de vous identifier.
http://home.free.fr/protection/enfance.html

Aol
Une fois que vous vous êtes connecté à l'univers AOL, vous trouverez l'option contrôle parental dans la barre de navigation (en haut de la page). Cliquez sur « contrôle parental » et finissez l'installation du logiciel (le logiciel est déjà pré-installé).
http://aolassistance.aol.fr/assistance/support/resultSearchKeyword.do?query=contr%F4le%20parental

Neuf
Pour trouver l'option contrôle parental, vous devez aller sur le site www.neufsecurite.fr. Cliquez sur « contrôle parental gratuit », puis sur « Pour accéder au Contrôle Parental gratuit de Neuf, cliquez ici ». Pour recevoir le logiciel, vous devez vous identifier. Vous recevrez un email avec un lien permettant de télécharger le logiciel ainsi que la clé d'activation du logiciel.
http://www.neufsecurite.fr/Neuf-Securite/controleparental.html#solution
http://www.neufsecurite.fr/Neuf-Securite/controleparentalform.html

Noos
Pour trouver l'option contrôle parental, cliquez sur « Protection de l'enfance » en bas de la page d'accueil. Ensuite, cliquez sur « Pour en savoir plus sur l'option Contrôle Parental, cliquez ici » en bas de la page dédiée à la protection de l'enfance.
http://www.lecable.fr/offre/offre_internet_option_controle_parental.php
http://www.noos.fr/assistance_en_ligne/assistance_net/les_servicess_et_options.php#2

Orange
Pour trouver l'option contrôle parental , cliquez sur « contrôle parental » dans la rubrique « Pratique » en bas à gauche de la page d'accueil. Ensuite cliquez sur « Installer le Contrôle Parental version 4.1 » à gauche de la page. Vous n'avez pas besoin de vous identifier.
http://www.orange.fr/bin/frame.cgi?u=http://assistance.orange.fr/755.php

Tele 2
Pour trouver l'option contrôle parental, allez sur www.tele2internet.fr et cliquez sur « GRATUIT ! Téléchargez le logiciel de contrôle parental de Tele 2 ». Le téléchargement se fait automatiquement. Vous n'avez pas besoin de vous identifier.
http://www.editorial.tele2internet.fr/?page=T2IPROM_CONTPAR

Astuces et liens divers

Virus, troyens, spyware :

Assiste.COM : www.assiste.com
Secuser : www.secuser.com
Securite.ORG : www.securite.org
SecuriteInfo : www.securiteinfo.com
ABC de la Sécurité : abcdelasecurite.free.fr/

Sites traitant de vulnérabilités :

CERTA : www.certa.ssi.gouv.fr
CERT-IST : www.cert-ist.com
RENATER : www.cri.uhp-nancy.fr/secinfo/index.php?id_rub=7&id_ssrub=41
US CERT : www.us-cert.gov
Secunia : secunia.com
Security Focus : www.securityfocus.com
Security Tracker : www.securitytracker.com
Microsoft Technet : www.microsoft.com/france/technet/securite/
FrSIRT : www.frsirt.com
Secuser : www.secuser.com/communiques/index.htm

Information autour de la sécurité :

IXUS : www.fr.ixus.net
ZATAZ : www.zataz.com
Vulnerabilite.COM : www.vulnerabilite.com
CLUSIF : www.clusif.asso.fr
The Register : www.theregister.com/security/
Le Blog du MSRC (Microsoft) : blogs.technet.com/msrc/
Sebsauvage.net : sebsauvage.net/safehex.html
LesNouvelles.Net : www.lesnouvelles.net
Branchez-vous.com : www.branchez-vous.com
SecuNews : www.secunews.org
ToutPourLePC : www.tplpc.com/modules/news/article-cat-0017.html
Secuser.com : http://www.secuser.com/ *(également l'un des meilleurs sites d'information sur les virus et failles en tout genre.)*
Trend micro : http://housecall.trendmicro.com/fr/
Panda software : http://www.pandasoftware.com/activescan/fr/activescan_principal.htm

Anti-virus / Pare-feu

Avast est un très bon antivirus gratuit.
ZoneAlarm est un pare-feu très performant et gratuit.

Tester son pare-feu :
Ce lien permet de tester son pare feu afin de vérifier que les réglages effectués permettent d'être invisible sur le réseau : http://www.zebulon.fr/outils/scanp

Anti-espion / Antispyware

Spybot est un des meilleurs antispywares, libre, gratuit et en français.
Ad-Aware est un autre antispyware, à utiliser en complément de Spybot.

Nettoyer son PC

CCleaner est un logiciel très performant qui permet de nettoyer un PC, en supprimant les fichiers temporaires, les erreurs...

Réaliser un scan en ligne d'un fichier en particulier

Jotti's malware scan (Lien communiqué par Ricricbe) : http://virusscan.jotti.org/

Liens vers les sites des fabricants d'antivirus

Antivir : http://www.avira.com/en/pages/index.php
Symantec : http://www.symantec.com/index.jsp
McAfee : http://www.mcafee.com/us/
Kaspersky : http://www.kaspersky.com/
F-secure : http://www.f-secure.com/
Panda software : http://www.pandasecurity.com/france/
Trend Micro : http://fr.trendmicro.com/fr/home/
Nod 32 : http://www.eset.com/
Avast : http://www.avast.com/index_fre.html

Encyclopédie des Virus

Viruslist.com (en français) : http://www.viruslist.com/fr/index.html

Navigateur pour Enfant

AmiWeb Personnel 3.0 : *Navigateur internet pour enfants de 4 à 9 ans.*
http://www.zdnet.fr/telecharger/windows/fiche/0,39021313,11008560s,00.htm
AmiWeb permet aux enfants de 4 à 9 ans de se familiariser avec internet en toute sécurité. Les parents choisissent les sites adaptés à chacun de leurs enfants. Une fois lancé, ce navigateur bloque l'accès aux autres programmes. Plus de risque de voir des données effacées

.